UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/797,767	03/10/2004	Patrick J. Helland	MS307035.1/MSFTP566US	4181

27195 7590 02/23/2009

AMIN, TUROCY & CALVIN, LLP
127 Public Square
57th Floor, Key Tower
CLEVELAND, OH 44114

EXAMINER
MORAN, RANDAL D

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
02/23/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket1@thepatentattorneys.com
hholmes@thepatentattorneys.com
lpasterchek@thepatentattorneys.com

Office Action Summary	Application No.	Applicant(s)	
	10/797,767	HELLAND ET AL.	
	Examiner	Art Unit	
	RANDAL D. MORAN	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 November 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-11,14-16 and 18-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-11,14-16,18-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-3, 5-11, and 14-16, and 18-28 are pending in the application.

This Office Action is in response to amendment filed 11/05/2008.

Below, Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully each reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Claim Rejections - 35 USC § 112

The rejection of **Claim 22** is withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-5, 9, 10, and 12- 21, 26, and 27rejected under 35 U.S.C. 103(a) as being unpatentable over **Stallings, William. *Cryptography and Network Security; Third Edition.* Chapter 9 / Public-Key Cryptography: 9.1: Principles of Public-Key Cryptosystems. Upper Saddle River, NJ. Prentice Hall, 2003. Pgs. 259-265, 290-293, 444, and 655.** Hereafter "Stallings" in view of **Bentley et al. (US 2003/0217275),** hereafter "Bentley."

Considering **Claim 1,** Stallings discloses a message encryption system (p.260- lines 28-36, p. 265- Figure 9.4) comprising: a session key employed to securely exchange a message associated with a dialog (p. 265- lines 18-19); and, an encryption component that employs asymmetric encryption to first securely transmit the session key (p. 292- lines 23-27, p. 293- lines 1-11, Fig. 10.6- (4)), the session key thereafter being employed to encrypt the message and securely exchange the message (p. 444- lines 19-21, p.655- line 21) , wherein the session key encrypted message is further encrypted using a private key securely associated with an initiator of the message (p. 265 - lines 15-17), the message is employed as part of a broker service security system that facilitates location transparency of services by creating a remote service binding such that an application can utilize the service independent of the physical location of the service (p. 264- lines 18-23, p. 265- lines 1-2, Fig. 9.4- item Z, according the instant specification [0124] from the PG Pub US 2005/0204139, creating of the remote binding only requires the initiator to determine that the target public key will be used to authenticate the connection. In Fig. 9.4, the public key of the target is further used to encrypt the message).

Stallings does not explicitly disclose a digital certificate which addresses a service by its logical name.

Bentley discloses a digital signature which addresses a service by its logical name ([0090]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Stallings by a digital; certificate that addresses a service by a logical name as taught by Bentley for the benefit of streamlining the process of creating signatures and improving quality control (Bentley [0090]).

Considering **Claim 14,** the combination discloses a message decryption system (p. 260- lines 25-36, p. 265- Fig. 9.4) comprising: a session key employed to securely exchange a message associated with a dialog (p. 265- lines 18-19); and, a decryption component that employs asymmetric decryption to first securely decrypt the session key (p. 292- lines 23-27, p. 293- lines 1-11), the session key thereafter being employed to decrypt the message (p. 444- lines 19-21, p. 655- lines 21) , wherein the session key encrypted message is further encrypted using a private key securely associated with an initiator of the message (p. 265 - lines 15-17), the message comprises a digital certificate (Bentley – [0090]) is employed as part of a broker service security system that facilitates location transparency of services by creating a remote service binding such that an application can utilize the service independent of the physical location of the service (p. 264- lines 18-23, p. 265- lines 1-2, Fig. 9.4- item Z, according the instant specification [0124] from the PG Pub US 2005/0204139, creating of the remote binding

only requires the initiator to determine that the target public key will be used to authenticate the connection. In Fig. 9.4, the public key of the target is further used to encrypt the message).

Considering **Claims 18 and 21,** the combination discloses a method facilitating session key encryption comprising (p. 444- lines 19-21): firstly encrypting a symmetric session key with a private key (p. 264- lines 18-23); secondly encrypting a result of the first encryption with a public key (p. 264- lines 18-23, p. 265- lines 1-2); and, providing a result of the second encryption as an output (p .265- Fig. 9.4- item Z), the output comprises a digital certificate (Bentley [0090]) is employed as part of a broker service security system that facilitates location transparency of services by creating a remote service binding such that an application can utilize the service independent of the physical location of the service (p. 264- lines 18-23, p. 265- lines 1-2, Fig. 9.4- item Z, according the instant specification [0124] from the PG Pub US 2005/0204139, creating of the remote binding only requires the initiator to determine that the target public key will be used to authenticate the connection. In Fig. 9.4, the public key of the target is further used to encrypt the message).

Considering **Claim 26,** the combination discloses a computer readable medium encoded with a data structure that facilitates secure distributed communication, the data packet comprising: a data field comprising an encrypted message, the encrypted message first encrypted with a symmetric session key (p. 265- Fig. 9.4), then encrypted with a private key securely associated with an initiator of the message (p. 265 - lines 15-17), the message comprises a digital certificate (Bentley [0090]) is employed as part of

a broker service security system that facilitates location transparency of services by creating a remote service binding such that an application can utilize the service independent of the physical location of the service (p. 264- lines 18-23, p. 265- lines 1-2, Fig. 9.4- item Z, according the instant specification [0124] from the PG Pub US 2005/0204139, creating of the remote binding only requires the initiator to determine that the target public key will be used to authenticate the connection. In Fig. 9.4, the public key of the target is further used to encrypt the message).

Considering **Claim 27,** the combination discloses a message decryption system (p. 260- lines 25-36, p. 265- Fig. 9.4) comprising: means for receiving an encrypted session key (p. 264- lines 18-23, Fig. 9.4- item Z); means for decrypting the encrypted session key using a private key (p. 264- lines 18-23, p. 265- lines 1-2, Fig. 9.4); means for decrypting a result of the first decryption with a public key (p. 265- Fig. 9.4); means for securely storing a result of the second decryption as a session key (p. 292- lines 23-27, p. 293- lines 1-11, Fig. 10.6- (4)); and, means for employing the session key to decrypt a message (p. p. 444- lines 19-21, p. 655- line 21) , wherein the session key encrypted message is further encrypted using a private key securely associated with an initiator of the message (p. 265 - lines 15-17), means for employing a digital certificate included in the message (Bentley – [0090]) creating a remote service binding such that an application can utilize the service independent of the physical location of the service (p. 264- lines 18-23, p. 265- lines 1-2, Fig. 9.4- item Z, according the instant specification [0124] from the PG Pub US 2005/0204139, creating of the remote binding only requires the initiator to determine that the target public key will be used to

authenticate the connection. In Fig. 9.4, the public key of the target is further used to encrypt the message).

Considering **Claim 2,** the combination discloses the session key comprising a 128-bit randomly generated symmetric key (Stallings p. 444- lines 19-30).

Considering **Claim 3,** the combination discloses the encryption component first encrypts the session key employing a private key (Stallings p. 264- lines 18-23); the encryption component further encrypts the result of the first encryption employing a public key (Stallings p. 264- lines 18-23, p. 265- lines 1-2).

Considering **Claim 19,** the combination discloses the private key being securely associated with an initiator of the message (Stallings p. 265- Fig. 9.4).

Considering **Claims 5 and 20,** the combination discloses the public key being associated with a target of the message (Stallings p. 265- Fig. 9.4).

Considering **Claim 9,** the combination discloses the public key being stored as a digital certificate (Stallings p. 260- lines 30-32, p. 261- Fig. 9.1- Bob's Public Key Ring).

Considering **Claim 10,** the combination discloses the digital certificate being associated with a user via a login protocol (Stallings p. 290, p. 291- lines 1-11).

Considering **Claim 13,** the combination discloses a broker security system employing the session key of claim 1 (Stallings p.260- lines 28-36, p. 265- Figure 9.4).

Considering **Claim 15,** the combination discloses the decryption component first decrypts a message with a private key (Stallings p. 264- lines 18-23, p. 265- lines 1-2), the decryption component further decrypting the result of the first decryption with a

public key (Stallings p. 265- Fig. 9.4), the result of the second decryption is the session key (Stallings p. 265- lines 5-19).

Considering **Claim 16,** Stallings discloses the private key being securely associated with a target of the message (Stallings p. 265- Fig. 9.4).

Considering **Claim 17,** the combination discloses the public key being associated with an initiator of the message (Stallings p. 265- Fig. 9.4).

2. **Claim 11** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Stallings and Bentley**.

Considering **Claim 11,** the combination discloses the encryption component first encrypts the session key employing a private key (p. 264- lines 18-23), the encryption component further encrypts the result of the first encryption employing a public key (p. 264- lines 18-23, p. 265- lines 1-2, p. 265- Fig. 9.4), and, the encryption component separately encrypts the session key with a public key (p. 260- lines 28-28, p. 261- Fig. 9.1), the result of the second encryption and the separate encryption provided as an output (Fig. 9.1, Fig. 9.4).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the techniques of the essential elements of public key encryption with the more advanced techniques of confidentiality, secrecy, and authenticity to produce two outputs for the benefit of further increasing the security of the session key transfer (p. 265- lines 5-19).

3. **Claims 6-8 and 22-25** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stallings and Bentley** in view of **VanHeyningen et al. (US 2002/0112152),** hereafter "VanHeyningen".

Considering **Claim 6,** Stallings and Bentley does not explicitly disclose a plurality of trusted agents that act as a proxy for a publisher to respectively exchange the message with respective subscribers, the trusted agents employing the private key. VanHeyningen discloses a plurality of trusted agents that act as a proxy for a publisher to respectively exchange the message with respective subscribers ([0092] lines 1-10, [0139] lines 1-8, Fig. 7B), the trusted agents employing the private key ([0039], [0095]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Stallings by a plurality of trusted agents that act as a proxy for a publisher to respectively exchange the message with respective subscribers, the trusted agents employing the private key as taught by VanHeyningen in order to avoid individually delivering messages to each appropriate recipient device in the network (e.g. point-to-point messaging), as this type of communication restricts the speed and efficiency of the invention (VanHeyningen- [0139] lines 1-8).

Considering **Claim 7,** the combination discloses a trusted agent negotiates a unique session key with a subscriber (VanHeyningen- [0039], [0095]).

Considering **Claim 8,** the combination discloses the trusted agents acting in concert to dynamically load balance distribution for the publisher VanHeyningen ([0091] lines 7-12, Fig. 7B- item 704).

4. **Claim 28** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Stallings and Bentley** in view of **Wasilewski et al. (US 5,870,474),** hereafter "Wasilewski".

Considering **Claim 28,** Stallings and Bentley does not explicitly disclose comprising multiple instances of the broker service sharing the same private key such that the application treats the multiple instances collectively as a unit.
Wasilewski discloses comprising multiple instances of the broker service sharing the same private key such that the application treats the multiple instances collectively as a unit (column 22- lines 13-34).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Stallings and VanHeyningen by deploying multiple instances of the service providers sharing the same private key to provide a system where the STU's (targets) would be unable to distinguish between service providers (initiators) (Wasilewski- column 22- lines 13-34).

5. **Claims 22-25** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stallings, Bentley** and **VanHeyningen** in view of **Wasilewski.**

Considering **Claims 22 and 25,** the combination discloses a method facilitating session key decryption comprising (p. 265- lines 18-19, p. 444- lines 19-21): firstly decrypting a message with a private key (p. 264- lines 18-23, p. 265- lines 1-2); second decrypting a result of the first decryption with a public key (p. 265- Fig. 9.4); and, employing a result of the second decryption as a session key (p. 265- lines 5-19), the session key thereafter being employed to decrypt the message, wherein the session

key encrypted message is first decrypted using a public key securely associated with an initiator of the message (Fig. 9.4); facilitating location transparency of services within a service broker security system employing the message by creating a remote service binding such that an application can utilize the service independent of the physical location of the service; (p. 264- lines 18-23, p. 265- lines 1-2, Fig. 9.4- item Z, according the instant specification [0124] from the PG Pub US 2005/0204139, creating of the remote binding only requires the initiator to determine that the target public key will be used to authenticate the connection. In Fig. 9.4, the public key of the target is further used to encrypt the message); and negotiating a unique session key with each of a subscriber accessing an instance of the service broker (VanHeyningen- [0039], [0095]). The combination does not explicitly disclose deploying multiple instances of the service broker; sharing the private key within the multiple instances of the service broker. Wasilewski discloses deploying multiple instances of the service broker; sharing the private key within the multiple instances of the service broker (column 22- lines 13-34).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Stallings and VanHeyningen by deploying multiple instances of the service providers sharing the same private key to provide a system where the STU's (targets) would be unable to distinguish between service providers (initiators) (Wasilewski- column 22- lines 13-34).

Considering **Claim 23,** the combination discloses the private key being securely associated with a target of the message (Stallings- p. 265- Fig. 9.4).

Considering **Claim 24,** the combination discloses the public key being associated with an initiator of the message (Stallings- p. 265- Fig. 9.4).

Response to Arguments

Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/R. D. M./
Examiner, Art Unit 2435
02/12/2009

/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2435